CLAIMS

What is claimed is:

1. In a client device equipped with a digital rights management system (DRM), a method comprising:

receiving a digital certificate associating an arbitrary digital action with a selected one or more of a plurality of secure components to facilitate performance of the digital action on protected content by the client;

verifying whether the digital certificate is authentic;

determining whether the client is authorized to perform the digital action; and

performing the digital action via execution of the one or more secure components if the digital certificate is authentic and the client is authorized to perform the requested action.

2. The method of claim 1, wherein determining whether the client is authorized to perform the digital action comprises determining whether a rights object associated with the protected content authorizes performance of the requested digital action based upon a rights expression corresponding to the DRM.

3. The method of claim 1,wherein each of the selected one or more secure components is associated with a corresponding unique identifier and the digital certificate contains unique identifiers corresponding to each of the selected one or more secure components.

4. The method of claim 3, further comprising determining whether each of the selected one or more secure components are stored on the client.

5. The method of claim 4, further comprising dynamically obtaining those of the selected one or more secure components stored external to the client.

6. The method of claim 1, wherein the digital certificate comprises a digital signature signed by a trusted third-party using a root encryption key belonging to a content provider source of the protected content.

7. The method of claim 6, wherein verifying whether the digital certificate is authentic comprises the client validating the digital signature of the digital certificate.

8. The method of claim 6, wherein the digital certificate is received in response to a request by the client to perform the digital action.

9. The method of claim 8, wherein the digital action comprises a selected one of a transcoding of the secure content, and a transfer of the protected content to another device.

10. The method of claim 1, wherein protected content comprises one or more content objects encrypted with components of a rights expression language of the DRM.

11. The method of claim 10, wherein the DRM is implemented in tamper resistant code.

12. The method of claim 1, further comprising receiving a digital rights object generated by a rights issuer associated with the secure content.

13. The method of claim 12, wherein the digital rights object comprises a license.

14. The method of claim 12, wherein the digital rights object is automatically received from the rights issuer.

15. The method of claim 12, wherein the digital rights object is received from the rights issuer in response to a user request.

16. The method of claim 15, wherein the user request is initiated via a user input device associated with the client.

17. A method comprising:

generating a plurality of secure components to facilitate performance of one or more digital content related actions by a client device;

generating a digitally signed certificate associating an arbitrary digital action with a selected one or more of the plurality of secure components; and

providing the digital certificate to the client.

18. The method of claim 17, further comprising:

generating a rights object corresponding to a digital rights management system (DRM) designed to facilitate performance of at least a subset of the one or more digital content related actions by the client device; and

providing the rights object to the client device.

19. The method of claim 18, wherein the rights object comprises a content license.

20. The method of claim 17, wherein each of the plurality of secure components is associated with a corresponding unique identifier and the digital certificate contains unique identifiers corresponding to each of the selected one or more secure components.

21. The method of claim 20, further comprising:

providing the selected one or more of the plurality of secure components to the client.

22. A machine readable medium having stored thereon machine executable instructions, which when executed by a client device equipped with a digital rights management system (DRM), operate to implement a method comprising:

receiving a digital certificate associating an arbitrary digital action with a selected one or more of a plurality of secure components to facilitate performance of the digital action on protected content by the client;

verifying whether the digital certificate is authentic;

determining whether the client is authorized to perform the digital action; and

performing the digital action via execution of the one or more secure components if the digital certificate is authentic and the client is authorized to perform the requested action.

23. The machine readable medium of claim 22, wherein determining whether the client is authorized to perform the digital action comprises determining whether a rights object associated with the protected content authorizes performance of the requested digital action based upon a rights expression corresponding to the DRM.

24. The machine readable medium of claim 22,wherein each of the selected one or more secure components is associated with a corresponding unique identifier and the digital certificate contains unique identifiers corresponding to each of the selected one or more secure components.

25. The machine readable medium of claim 24, further comprising instructions to determine whether each of the selected one or more secure components are stored on the client.

26. The machine readable medium of claim 25, further comprising instructions to dynamically obtain those of the selected one or more secure components stored external to the client.

27. The machine readable medium of claim 22, wherein the digital certificate comprises a digital signature signed by a trusted third-party using a root encryption key belonging to a content provider source of the protected content.

28. The machine readable medium of claim 27, wherein verifying whether the digital certificate is authentic comprises the client validating the digital signature of the digital certificate.

29. The machine readable medium of claim 27, wherein the digital certificate is received in response to a request by the client to perform the digital action.

30. The machine readable medium of claim 29, wherein the digital action comprises a selected one of a transcoding of the secure content, and a transfer of the protected content to another device.

31. The machine readable medium of claim 22, wherein protected content comprises one or more content objects encrypted with components of a rights expression language of the DRM.

32. The machine readable medium of claim 31, wherein the DRM is implemented in tamper resistant code.

33. The machine readable medium of claim 22, further comprising instructions to receive a digital rights object generated by a rights issuer associated with the secure content.

34. The machine readable medium of claim 33, wherein the digital rights object comprises a license.

35. The machine readable medium of claim 33, wherein the digital rights object is automatically received from the rights issuer.

36. The machine readable medium of claim 33, wherein the digital rights object is received from the rights issuer in response to a user request.

37. The machine readable medium of claim 36, wherein the user request is initiated via a user input device associated with the client.

38. A machine readable medium having stored thereon machine executable instructions, which when executed operate to implement a method comprising:

generating a plurality of secure components to facilitate performance of one or more digital content related actions by a client device;

generating a digitally signed certificate associating an arbitrary digital action with a selected one or more of the plurality of secure components; and

providing the digital certificate to the client.

39. The machine readable medium of claim 38, further comprising instructions to

generate a rights object corresponding to a digital rights management system (DRM) designed to facilitate performance of at least a subset of the one or more digital content related actions by the client device; and

provide the rights object to the client device.

40. The machine readable medium of claim 39, wherein the rights object comprises a content license.

41. The machine readable medium of claim 38, wherein each of the plurality of secure components is associated with a corresponding unique identifier and the digital certificate contains unique identifiers corresponding to each of the selected one or more secure components.

42. The machine readable medium of claim 41, further comprising instructions to provide the selected one or more of the plurality of secure components to the client.